CLAIMS:

1. A method for authenticating a transaction comprising the steps of:
presenting a nonce stamp having a nonce;
presenting a numbered digital certificate derived securely from the nonce; and
authenticating the transaction by comparing the number on the digital certificate and the nonce.

2. The method of Claim 1, wherein the nonce is represented on the nonce stamp within a bar code.

3. The method of Claim 1, wherein the digital certificate is marked on a physical medium.

4. The method of Claim 1, wherein the number on the digital certificate is represented within a two dimensional bar code.

5. The method of Claim 1, wherein the numbered digital certificate is derived by encrypting the nonce number.

6. The method of Claim 5, wherein comparing the number on the digital certificate and the nonce comprises encrypting the nonce, and matching the encrypted nonce against the number on the digital certificate.

7. The method of Claim 5, wherein comparing the number on the digital certificate comprises decrypting the number on the digital certificate and matching the decrypted number with the nonce.

8. The method of Claim 1, further comprising obtaining the digital certificate for a user by paying a purchase price for the transaction.

9. The method of Claim 8, wherein obtaining the digital certificate is performed remotely via an electronic communications network.

10. The method of Claim 9, wherein the user is in physical possession of the nonce stamp, and wherein obtaining the digital certificate for the user further comprises remotely transmitting the nonce.

11. The method of Claim 10, wherein obtaining the digital certificate further comprises deriving the number on the digital certificate by encrypting the nonce remotely transmitted for the user.

12. The method of Claim 11, wherein obtaining the digital certificate further comprises transmitting digital certificate information, including the number on the digital certificate, to the user via the electronic communications network.

13. The method of Claim 12, wherein obtaining the digital certificate further comprises receiving the digital certificate information and locally printing a tangible copy of the numbered digital certificate.

14. The method of Claim 8, wherein obtaining the digital certificate is performed using a tamper-resistant module at a system local to the user, the tamper-resistant storing user account information.

15. The method of Claim 14, wherein the user connects electronically to a remote vendor in order to purchase credit for the user account stored by the tamper resistant module.

16. The method of Claim 15, wherein the vendor remotely updates, via electronic network, the account information in the tamper-resistant module.

17. The method of Claim 1, wherein the numbered digital certificate further comprises a description of at least one element of the transaction selected from the group consisting of purchase price, purchased product/service, transaction authority.

18. The method of Claim 1, wherein the nonce stamp and the numbered digital certificate are physically coupled together.

19. The method of Claim 18, wherein the numbered digital certificate is printed on the nonce stamp.

20. The method of Claim 1, wherein the nonce stamp and the numbered digital certificate are physically coupled to an article of the transaction.

21. The method of Claim 1 wherein the transaction comprises depositing an article of mailing, and the method further comprises presenting the nonce stamp and the numbered digital certificate as postage for the article of mailing.

22. The method of Claim 1 wherein the transaction comprises admission to a facility, and the method further comprises presenting the digital certificate and the nonce stamp as a ticket for admission to the facility.

23. An information-based indicium for authenticating a desired transaction, comprising:

a) a nonce stamp comprising a nonce; and

b) a digital certificate comprising a number derived securely from the nonce;

wherein the digital certificate and the nonce stamp may be presented together to authenticate the transaction by comparing the number on the digital certificate and the nonce.

24. The information-based indicium of Claim 23, wherein the nonce is represented on the nonce stamp within a bar code.

25. The information-based indicium of Claim 23, wherein the digital certificate is marked on a physical medium.

26. The information-based indicium of Claim 23, wherein the number on the digital certificate is represented within a two dimensional bar code.

27. The information-based indicium of Claim 23, wherein the numbered digital certificate is derived by encrypting the nonce.

28. The information-based indicium of Claim 27, wherein comparing the number on the digital certificate and the nonce comprises encrypting the nonce, and matching the encrypted nonce against the number on the digital certificate.

29. The information-based indicium of Claim 23, wherein the numbered digital certificate further comprises a description of at least one element of the transaction selected from the group consisting of purchase price, purchased product/service, and transaction authority.

30. The information-based indicium of Claim 23, wherein the nonce stamp and the numbered digital certificate are physically coupled together.

31. The information-based indicium of Claim 23, wherein the numbered digital certificate is printed on the nonce stamp.

32. The information-based indicium of Claim 23, wherein the nonce stamp and the numbered digital certificate are physically coupled to an article of the transaction.

33. The information-based indicium of Claim 23 wherein the transaction comprises depositing an article of mailing, and the information-based indicium comprises postage for the article of mailing.

34. The information-based indicium of Claim 23 wherein the transaction comprises admission to a facility, and the information-based indicium comprises a ticket for admission to the facility.

35. A system for generating information-based indicia for a user's desired transaction, comprising one or more computers configured to:

a) receive as input a nonce from a nonce stamp of the user;

b) encrypt the nonce; and

c) provide to the user a digital certificate comprising the encrypted nonce,

whereby the nonce stamp and the digital certificate may be collectively presented as an information-based indicium for the desired transaction.

36. The system of Claim 35, wherein the one or more computers are further configured to specify a user's desired transaction, and to charge the user a transaction price for the desired transaction.

37. The system of Claim 36, wherein the computers are configured to charge the user prior to providing the digital certificate to the user.

38. The system of Claim 36, wherein the computers are configured to receive the nonce, encrypt the nonce, specify the desired transaction, charge the user, and to provide the digital certificate, at least partly through remote interaction between the user and a vendor across one or more electronic communication networks.

39. The system of Claim 38, wherein the remote interaction is conducted between client browsing software of the user and an Internet site of the vendor.

40. The system of Claim 38, wherein the computers are configured to provide the digital certificate to the user by transmitting digital certificate information, including the number on the digital certificate, to the user via the electronic communications network.

41. The system of Claim 40, wherein the computers are further configured to provide the digital certificate to the user by receiving the digital certificate information at the user's end and locally printing a tangible copy of the digital certificate.

42. The system of Claim 36, wherein the one or more computers include a tamper-resistant module local to the user, and are configured to encrypt the nonce using the tamper-resistant module.

43. The system of Claim 42, wherein the tamper-resistant module stores user account information, and wherein the one or more computers are configured to charge the transaction price by using the tamper-resistant module to update the stored account information.

44. The system of Claim 43, wherein the tamper resistant module is intermittently coupled, via network, to a remote vendor who updates the stored account information to reflect credit purchased by the user.

45. The system of Claim 35, wherein the transaction comprises mailing an article of mailing and the information-based indicium comprises postage.

46. The system of Claim 35, wherein the transaction comprises gaining admission to a facility and the information-based indicium comprises an admission ticket.

47. An information-based indicium comprising:

a) a forgery-resistant physical article bearing an identification number;

b) a digital certificate including a number derived securely from the identification number;

wherein the information based indicium may be authenticated by comparing the number on the digital certificate and the identification number.

48. The information-based indicium of Claim 47, wherein the identification number is represented on the physical article in a human-readable form.

49. The information-based indicium of Claim 48, wherein the identification number is represented on the physical article in a form readable by standard image scanners.